Global Information Assurance Certification Paper

LAPTOP SECURITY: PAST, PRESENT

By
Andrew Mueller

The need for laptop security arose early on in the timeline of laptop evolution. The first time someone left their ten pound IBM Thinkpad running Windows 3.11 in the back of their car, only to return to a broken window and a missing laptop, the need for better protection arose. The luxury of portability that a laptop brought a user came at a price, the risk of having their computer compromised. The responsibility fell heavily on the user as well as on the organization. Companies struggled to not only protect the physical equipment but also the sensitive information stored on their laptops.

Through this need separate genres of security were created. The simplest is the physically protection of the laptop. This is technology that helps prevent the actually stealing of the laptop. Companies found however, that not everyone could be protected at all times, and eventually laptops would still get stolen. This prompted the revolution of data security. Data security represents the attempt to protect the user's data from malicious people after the laptop is stolen. This is different from other security solutions like firewalls and file encryption, which protects the data while the user is still in possession of their laptop and using it for their daily work. This paper will discuss the physical safety measures as well as post theft data protection.

Organizations found that the easiest and cheapest way to protect their investments were through education of their employees. Documents about how to handle yourself and your equipment while out on the road where developed. Most of these documents dealt solely with the user's responsibilities. For instance, as stated in the example above, avoid leaving your laptop in full view on your car seat.

Physical protection is the headwall of security for any platform, but it is especially important for laptop users. If a malicious person has physical access to any type of computer: desktop, server, home PC, laptop, etc. it makes things much easier for them to accomplish their goal. If their goal is to physically steal the piece of equipment to sell it for its hardware value, physical access to it, is obviously all they need. If they are looking to siphon data off it, or hack passwords, physical access will help them out greatly. If the hacker has physical access to the machine in question, they now have several more options than they would have if the system was locked behind a door in an office, house, or lab. The hacker can remove the hard drive to bring it home and hack at their leisure, not risking getting caught by the user. They can also just take the whole system and do the same thing. In many cases where security is a little lax in the computer setup, they

can boot to a floppy disk and attack the OS using various utilities, pulling password files onto floppy disks, using utilities such as NTFS-DOS, PWDump, SAMDump and many more. All these utilities are easily obtainable and such black hat hacker sites as http://www.censorfreeworld.com.

Users were educated early on to lock offices or labs as well as desktops cases. Servers and desktops were configured in their BIOS to not allow users to boot to floppies on them. The laptop users face several different challenges. Today for example, they are instructed to not let their laptop leave their sight when they are going through metal detectors at airports, which is a common place to have laptops stolen a risk a desktop user would never be exposed to.

Even with user education, organizations are still looking for ways to warn and protect their mobile work force from thieves and hackers. Companies such as PORT are making products to help users with the hardware security of their laptops. PORT offers laptop cases with motion detectors built into them. The idea is when someone puts their laptop bag down in an airport for example; they can arm their laptop bag. It comes with a remote control, so the user doesn't have to bend down and touch anything on their bag. Small movements of the bag are undetected but if the bag is actually picked up or moved, the alarm emits several short beeps. If you fail to disarm the alarm, or continue to walk with it, a very loud and obtrusive alarm sounds, until the bag is disarmed. PORT also offers another smaller motion detector security lock for the laptop. It is very similar to other security locks, which are used to fasten systems to desks in an office, however if the cable is moved too much, the alarm will sound. This is useful for users that do not want to buy the somewhat more expensive motion detector bag; they can buy the cable lock for less and attach it to their own bag.

The future of motion detection for laptops has been realized by companies like Caveo Technology. Their product is called Caveo Anti-Theft and it is a hardware/software solution. The hardware piece is a motion detector that will fit either directly on the motherboard, or possible in PCMCIA slots provided. A user will create a "password" based on movements of the laptop. For instance, your password could be: A 90 degree roll forward and then a 90 degree to the left side. Once done your system would then be usable.

If you attempt to move the laptop or if it was moved violently, for instance if someone grabbed it and ran off with it, the motion detector will be tripped and an alarm will sound. The software section of this piece sits between the BIOS and the Operating System, so as soon as the alarm is tripped the software makes the hard drive inaccessible. When you first load the software onto your laptop you set up an eight digit password through the application. If you have the password, you can than reset the alarm system, and get back into the Operating System.

Another piece of technology which is on the forefront of physical security is electronic asset identification. IBM has successfully implemented Asset ID into several of their

products. Asset ID is burned into the EEPROM of the system, and can be accessed through radio-frequency no matter if the system is powered on or off. When coupled with other products like Electronic Property-Pass and Asset Portal Reading it can be used as a physical security solution.

Scanners that look like metal-detectors can be placed at the exits of buildings, where normally security guards would be stationed. When a user steps through one of these scanners it reads the information on their Asset ID and compares that information to their identification badge. If the credentials do not match up, several things can be programmed to happen. An alarm can sound, or a message can be sent to a security guard or administrator. Other options are programmable into the software to help alert individuals when their equipment is leaving their building without the proper authorization.

It is said that the Department of Defense uses this type of set up to actually disable the drive if it appears to be leaving their buildings without proper authentication.

Another less, technical security advance in asset tracking is the property labeling of companies equipment to identify it clearly. This simply identification technology has actually progressed since its inception. Originally, an asset tag was placed on a system to mark it; however they were general easy to remove, or cover up. Companies like TechSaver developed a product called Stop Tag that are placed on laptops in the hopes of deterring theft, but these are much more difficult to take off. A sticker/plate is attached to the laptop with warnings that the laptop's possessor is constantly monitored and that resale of the laptop is impossible. According to TechSaver's website (which is sited in Appendix A) it takes eight hundred pounds of pressure to remove these tags. This works for the thieve who is after monetary gain by selling the hardware that they have stolen, but doesn't help much with the thief who is after the data.

These are all examples of manufacturers building products and solutions, as well as education users, to help stop the physical theft of a laptop. But what happens, when those measures are not in place, or perhaps gotten around by a persistent, most likely deaf, thief? How do you ensure that the new code you were working on does not end up posted on the internet for all to copy, two days after your laptop was stolen?

There are many companies currently working on answering these questions. When Microsoft® introduced their NTFS file system it was a step in the right direction. Malicious users could no longer access files from DOS boot-up disks. However, as is par for the White Hat vs. Black Hat community of security enthusiasts a utility was created, not too long afterwards, that allowed people to do just that. When NTFS-Dos was released it quickly made the limited security of NTFS even less impressive.

Companies like Symantec and Network Associates Incorporated (NAI) who were already providing virus solutions stepped into the ring. Symantec created a program called Your

Eyes Only and through an acquisition NAI bought Pretty Good Privacy (PGP). Both these products provided data encryption at the file level. Although a very good solution, there were still some security holes in that solution. What happened if the user forgot to encrypt important data, or forgot to place files into the encrypt–on-the-fly volumes? These measures would only be as good as the user's memory to use them.

Another company called PointSec (formerly Protect) came up with a disk encryption product that encrypted the complete hard drive, this helps solve some of these issues. Because the software runs below the Operating System, the hard drive is rendered inaccessible until the correct username and password are entered. The hard drive will stay in an inaccessible state even after it is physically pulled out of the system, unless the proper credentials are provided. This is a really effective tool to make sure that the data on your drive stays confidential even if your system is stolen.

These products that require a separate set of credentials to actually access the hard drive, from the set of credentials a user has to input to get through an Operating System authentication, have an exciting future ahead of them. Their future lies in the area of biometrics. Biometrics in the computer world is the replacement of a password you type in, with a feature from your body that is solely individual to you. The most obvious one is your fingerprint, but others include full face scans as well as optical readings, and voice recognition.

Companies such as Neurodynamics, BioNetrix, Identix, and many more, are heavily in the biometrics market. One of the most common biometrics solution is the fingerprint reader. A laptop is installed with a PCMCIA card that has a sleeve that ejects from the end of it. On that sleeve is a fingerprint reader. Simply put, the user places their finger on the reader, if the prints match up the user is granted access to the system. Although this technology is still relatively expensive, the price on this set up is slowly dropping, making this very tight security option a possible solution for more people in the future.

Digital cameras are making the ability to unlock your computer through facial recognition a reality. As the price points on all these products continue to drop the possibilities for wide spread biometric security systems for the mobile work force become more attainable.

There is an argument over what industry started the tracking and recovery of product, the automotive or the computer. Either way both employ some similar technologies at the core, and have just customized it to their specific needs. The basis behind tracking and recovery in the computer industry is to figure out a way that once a laptop is stolen it can be recovered by monitoring the location of where it connects to the internet or even simpler when a phone line has been plugged into it.

One company that is pioneering this technology is called Loss Prevention Services. They are an alarm-monitoring system and have developed software called LapTrack for laptop users. This software is totally invisible to a user unless they have the correct password to

launch its administrative software. If a laptop is stolen the software will silently try to contact the monitoring headquarters. It does this by either straight modem call, or if the system is connected to the internet, through for instance a LAN, it will connect to the monitoring station also.
It will continue to try and reach the call center until it finally gets through. The obvious drawbacks are that if the laptop is never connected to a modem line, or network with internet access, or even worse if the laptop is formatted the service will not work. The advantage of this method is if someone boots up a stolen laptop with this software running, the program will continually try to dial out. As soon as a telephone line is plugged into the system the call is made silently, with the user totally unaware. Once the information hits the call center they can start traces to determine the location of the laptop.

Another company with this same approach is Computrace. They too have the same advantages as LapTrack as well as their drawbacks, and their procedures are very similar. As stated above the major drawback of software based tracking is the threat of an operating system getting completely erased before the software has a chance to run. Both these companies as well as the other couple that provide this software and service have suggestions on how to minimize that risk.

Their suggestion is to change the boot order in the BIOS to make sure that the hard drive boots first and the floppy comes after that. Once that is done they also suggest password protecting the BIOS so that one cannot get into it to change the boot order back. This will most likely dissuade the thief from trying too hard to get into the BIOS and hopefully they will boot up the operating system at that point activating the software. However, if a thief is smart enough to know how to re-install an operating system, there is a chance that they may know about sites like http://www.hack-net.com or http://www.password-crackers.com which both offer many different utilities for cracking BIOS passwords.

As touched on above this brings up some challenges. Even if they do boot the operating system they will still at least have to plug in a phone line during this time. Certainly a big variable necessary for the success of this security method.

On a positive note these companies have had many cases of arrests using this combination of software and monitoring, as other documented successes from other companies that offer the same service. Every company is quick to display their testimonials and most have direct links off their homepage. In the appendix I have provided a list of links and both Computrace, and Loss Prevention Service are listed in the back, with both their homepages either linking to, or directly listing testimonials about their service. With the price ranging anywhere from $25-$55 a year per system, it might not be that bad of an investment for some companies.

In the end it comes down to the intelligence of the thief, the amount of computer experience they have, and the reason the laptop is stolen in the first place. The two reasons would be data recovery, the other to just sell the hardware. (I suppose a third

would be to use it themselves).

The future of this technology I believe will be a BIOS based service. Something hard-coded in the BIOS that will be used to track the laptop. The car industry uses a GPS satellite to track some of its more expensive automobiles and perhaps that is where the laptop industry will go.

The benefits that are created by the laptop industry are numerous. The ability for a user to work almost anywhere, at anytime has greatly increased productivity. With the advances in wireless becoming more and more prevalent in the laptop industry, people are able to remain connected in some of the most remote locations.

Along with these benefits, however come pitfalls and risks. Data is no longer secured behind a locked door, in a locked building, guarded by a security guard. Sensitive data is at times left in a laptop in the backseat of a car, or under a seat at an airport. The physical security advances discussed are proof that industries are listening to users concerns and working on solutions. PCMCIA fingerprint readers, fully encrypted disks and many other products are at the forefront of this industry.

The technology is driven by companies that are constantly trying to provide a more personally experience for the average laptop user. The future of security I think will mirror that process. We have already seen biometrics incorporated into computer security and I think the industry will run with that. Systems that won't even power up until the proper fingerprint is pressed against a scanner, or the proper eyeball is pressed against the lens, are not too far off, for the common employee.

Systems hard coded with small GPS tracking units will creep into the corporate world, and users will be able to track where their laptops are if they've been stolen, and recovery will be more and more common.

One can only speculate about the future of hardware security on a laptop. Perhaps looking to the movies will give us an idea of where we are going, since many things that we saw in 80's sci-fi movies are everyday occurrences nowadays. Retinal scanners, voice commands, voice passwords, and fingerprint scanners were all Hollywood inventions before they were actual technologies. Although following that line of reasoning may not be the best choice since it may lead to the discovery that we don't need any of these new and improved security measures at all, due to the fact that our whole existence is just one giant Matrix.

Appendix

Thanks to the following companies, for their product information. I learned a lot about security by perusing their sites. Although nothing was directly footnoted, these sites helped form my opinions and beliefs, and I couldn't have written this paper without the information I got at these internet sites.

PORT
http://www.port.com/accessories/security.asp

Network World Fusion
http://www.nwfusion.com/newsletters/mobile/2001/00477464.html

Pretty Good Privacy
http://www.pgp.com/products/disk-encryption/default.asp

PointSec
http://www.pointsec.com/solutions/solutions.asp

Neurodynamics
http://www.neurodynamics.com/BIOMETRICS/biometrics_home.htm

BioNetrix
http://www.bionetrix.com/products.htm

IBM
http://www5.pc.ibm.com/ww/me.nsf/ee8a81475a967409852569310062f304/b9b387e564b5517785256962006571 4d/$FILE/xbasset.PDF

The Business Journal
http://triad.bcentral.com/triad/stories/2000/10/16/newscolumn8.html

CompuTrace
http://www.computrace.com/index_abo_pro.asp#tracking

TechSaver
http://store.yahoo.com/secure-equipment/stoptags.html

Last Updated: July 24th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event